# Why signatures?

# Legal Conception of Signature

## General Purposes of Signing

- *Evidence*: a distinctive mark of the signer
- *Ceremony*: calls attention to the act
- *Approval*: implies approval and binding intent
- *Efficiency*: prima facie validation of the instrument (document)

# Legal Conception of Signature

## Requisite Attributes of Signatures

- *Signer Authentication*: proof of identity
- *Document Authentication*: proof of subject
- *Approval*: non-repudiable act should require conscious intervention
- *Efficiency*: provide maximum assurance with reasonable effort

**Contract Formation**

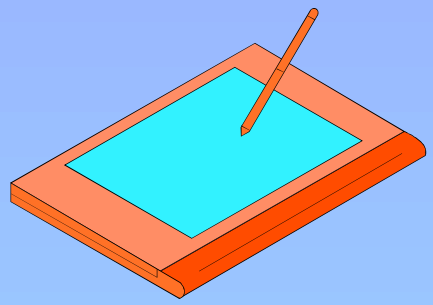
- A *physical act or ceremony* traditionally accompanies contract formation (e.g., handshake, signed document) to show intent to be bound
- Contracts may be formed *in any manner sufficient to show agreement*

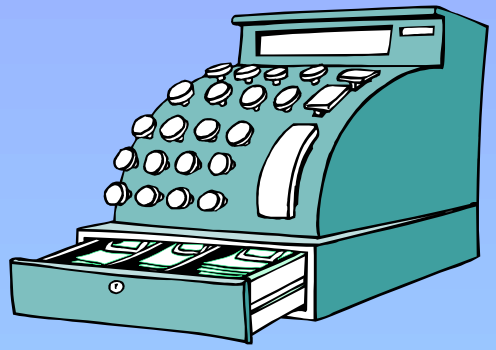
  (Electronic contracting replaces physical contact and cues with an exchange of *intangible bits of information* which can be reinforced with ceremony via interaction with other party or with the signing application)
- Contracts formed via *electronic signatures* can be valid and enforceable

# Current Electronic Signature Use

You sign a check **OR**

You “sign” an ATM withdrawal





You “sign” a debit/credit card purchase

**Secure system based signing processes - the proof is in the system.**

**Determining when to use a "signature" and what type.**

- Identify transactions that can be streamlined by becoming electronic events.

- Consider what the signature requirements for the transaction are.
  - Is there a need for a formal "legal" signature?
  - Will strong authentication of identity be enough? (via a password, PIN, etc)

The main push for electronic signatures now is for more formal needs. Financial transactions routinely occur now, but more contractual signings may need a process that is:

- more strongly linked to the person
- more durable - the signed record/document endures for the "legal" life of the contractual obligation.

## What is a “signature”?

Consider the reasons to use a *secure electronic signature*:

1. to identify the person signing
   (the identification function);

2. to indicate that person’s approval
   of the information contained in that data message
   (the authentication function);

3. to indicate that the record has not been altered
   (the integrity function).

Is that level of “signing” necessary?

## Arizona's simplified secure form of Electronic Signatures

An electronic signature

shall be unique to the person using it,

shall be capable of reliable verification and

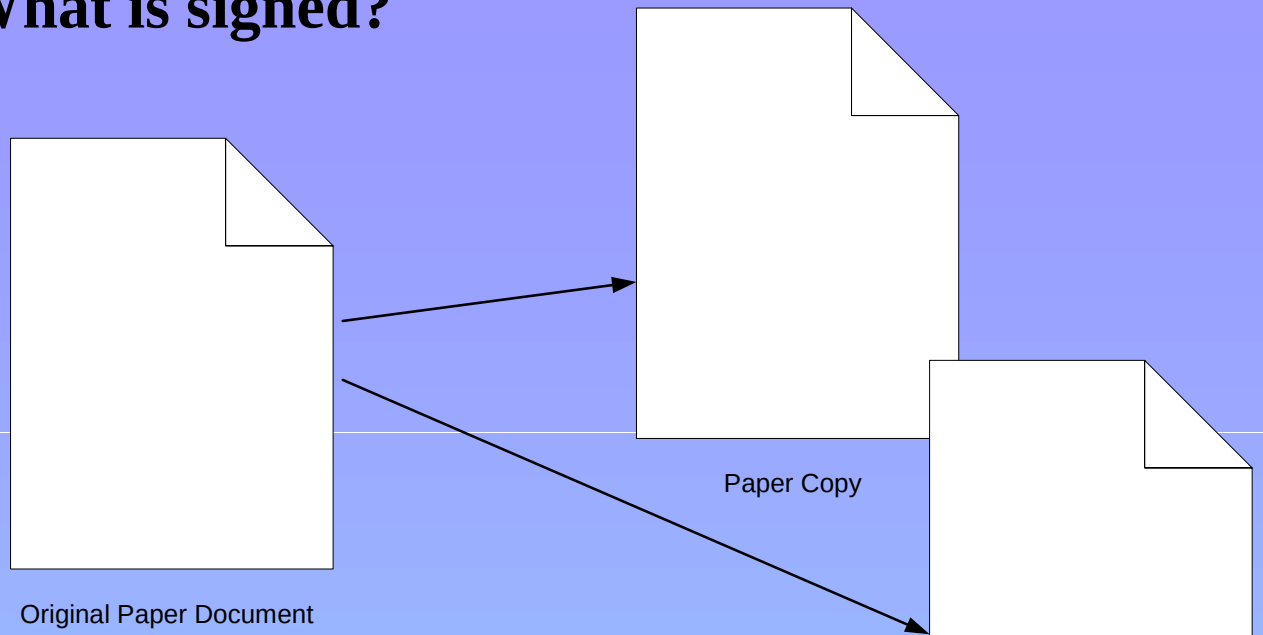
shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

Arizona Statute 41-132 B

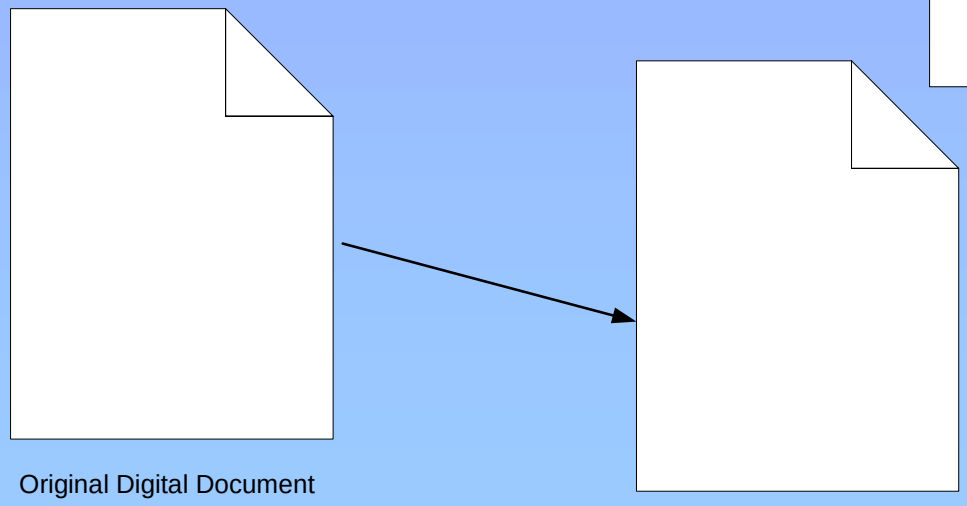
(*specific to signing by/with state agencies*)

# What is signed?

A copy of a paper document is a copy, whether it is another paper document or a digital image.

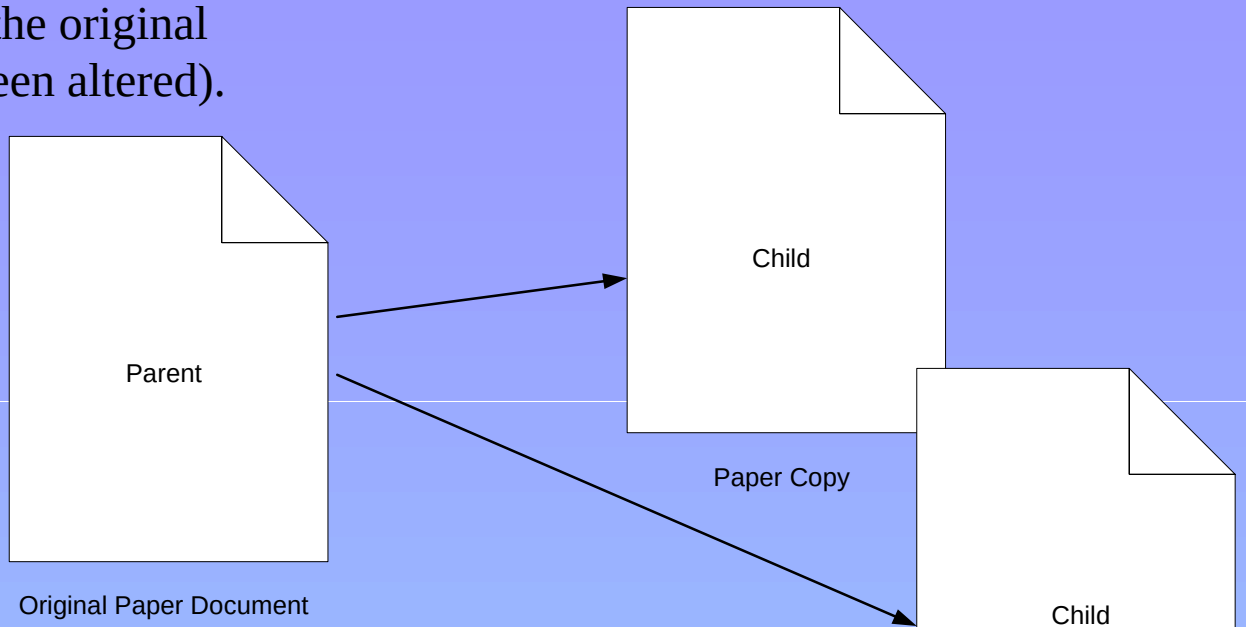



It is possible to send an original digital document to someone - while you keep the original of it.



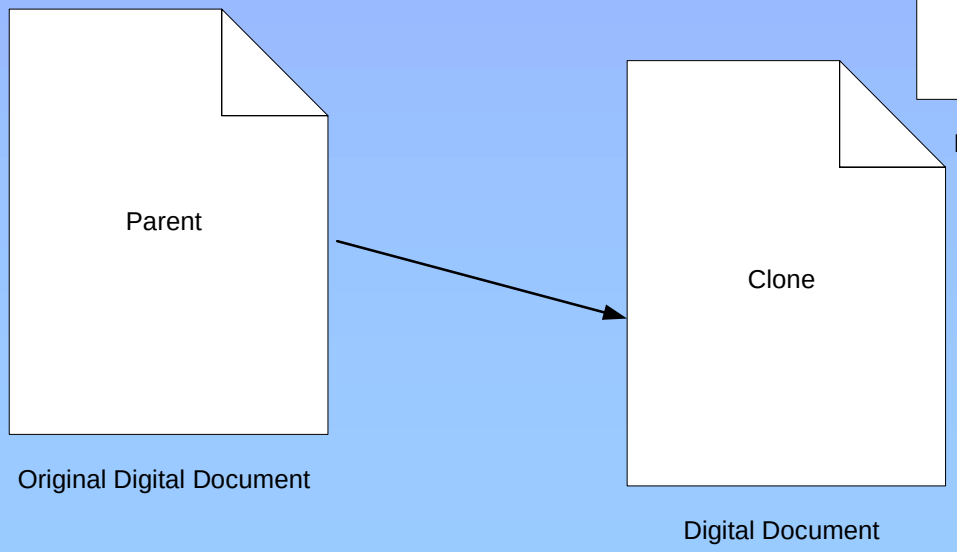

There is *no* difference between them!

The validity of a copy of a paper document depends on the validity of the original (and that the copy hasn't been altered).




The validity of a digital document depends on the tests it can pass - including whether it has been altered.

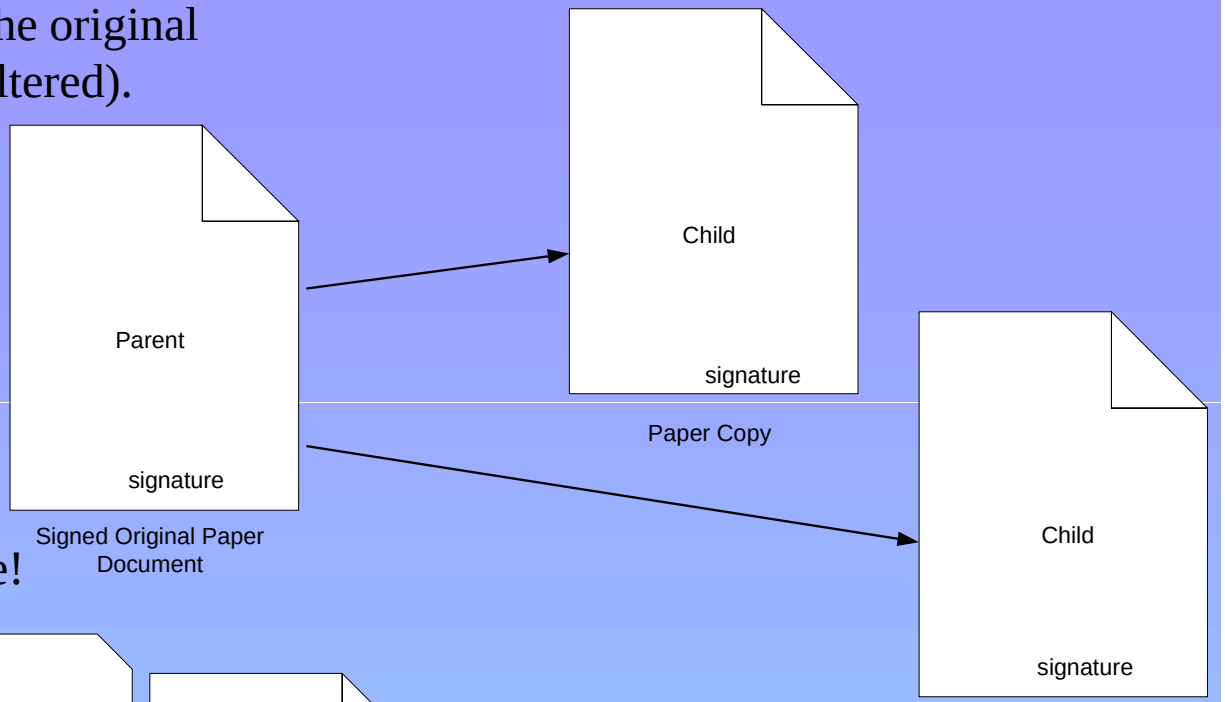
Since there is no copy, only a clone, those tests apply to the clone as well.

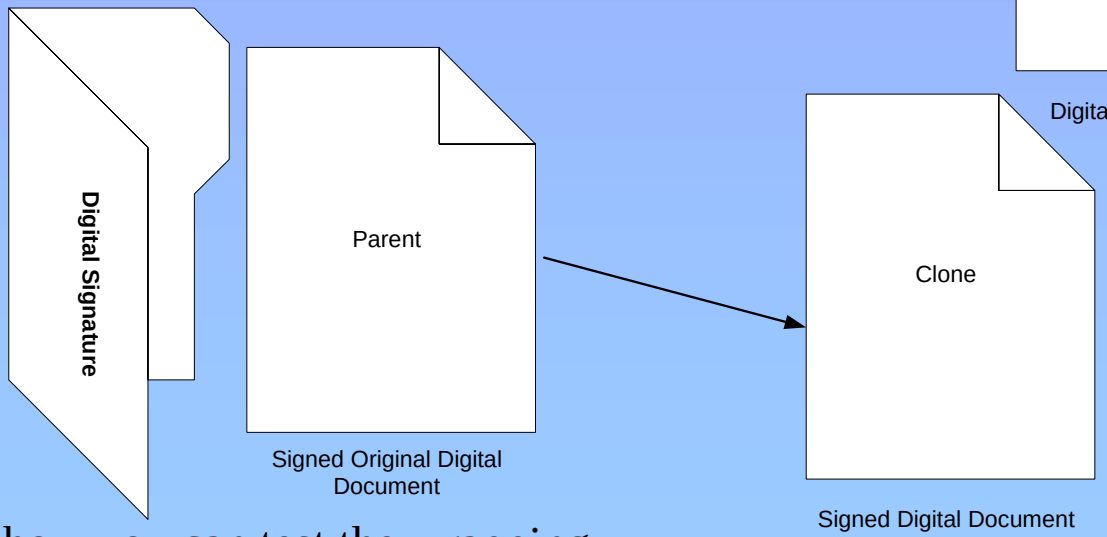


The validity of a copy of a signed paper document still depends on the validity of the original (and that the copy hasn't been altered).

There is the extra complication that you could sign a copy which would add "legal standing" to the copy.

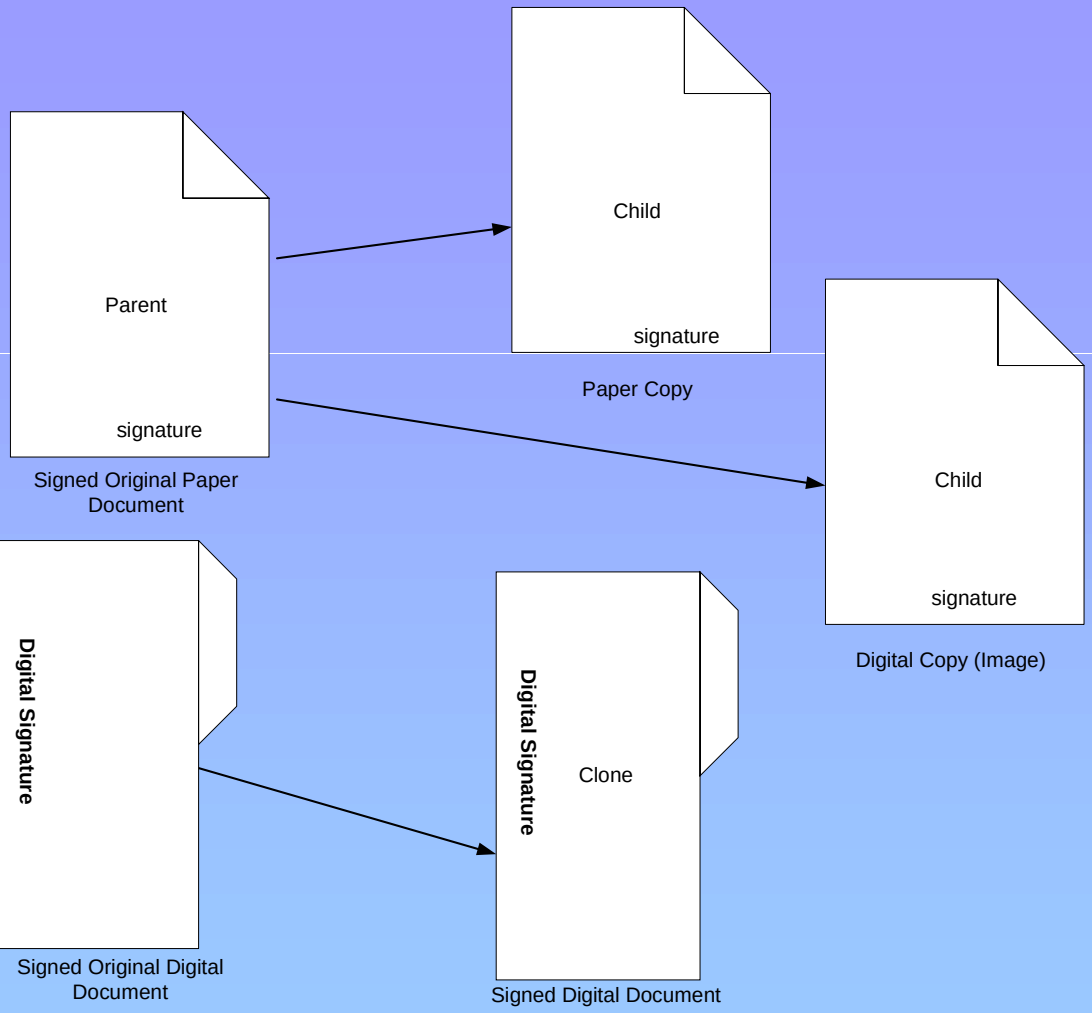
You could even make it a clone!




A digital signature wraps the document. The validity of the document depends on how you can test the wrapping such that its contents were not altered. The wrapper can be transparent or opaque.

Keeping a “legal” digital image of a paper original usually requires an affidavit or oath that it is a true, unaltered copy.



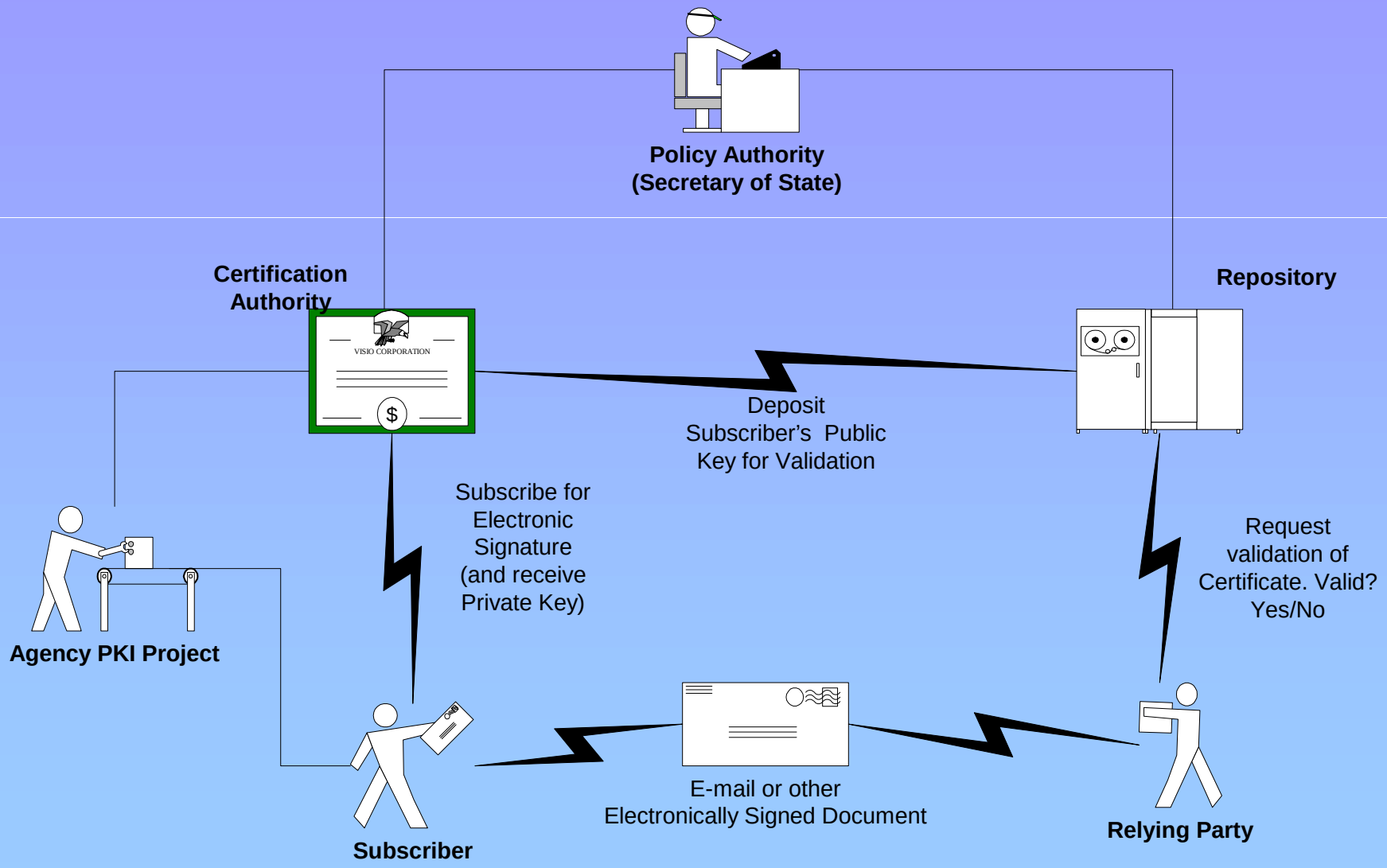

Keeping a “legal” digital document requires being able, over time,
to test the signature’s validity and the document integrity and keeping the document readable.

**Arizona's simplified secure form of Electronic Signatures is based on using PKI (digital signatures)**

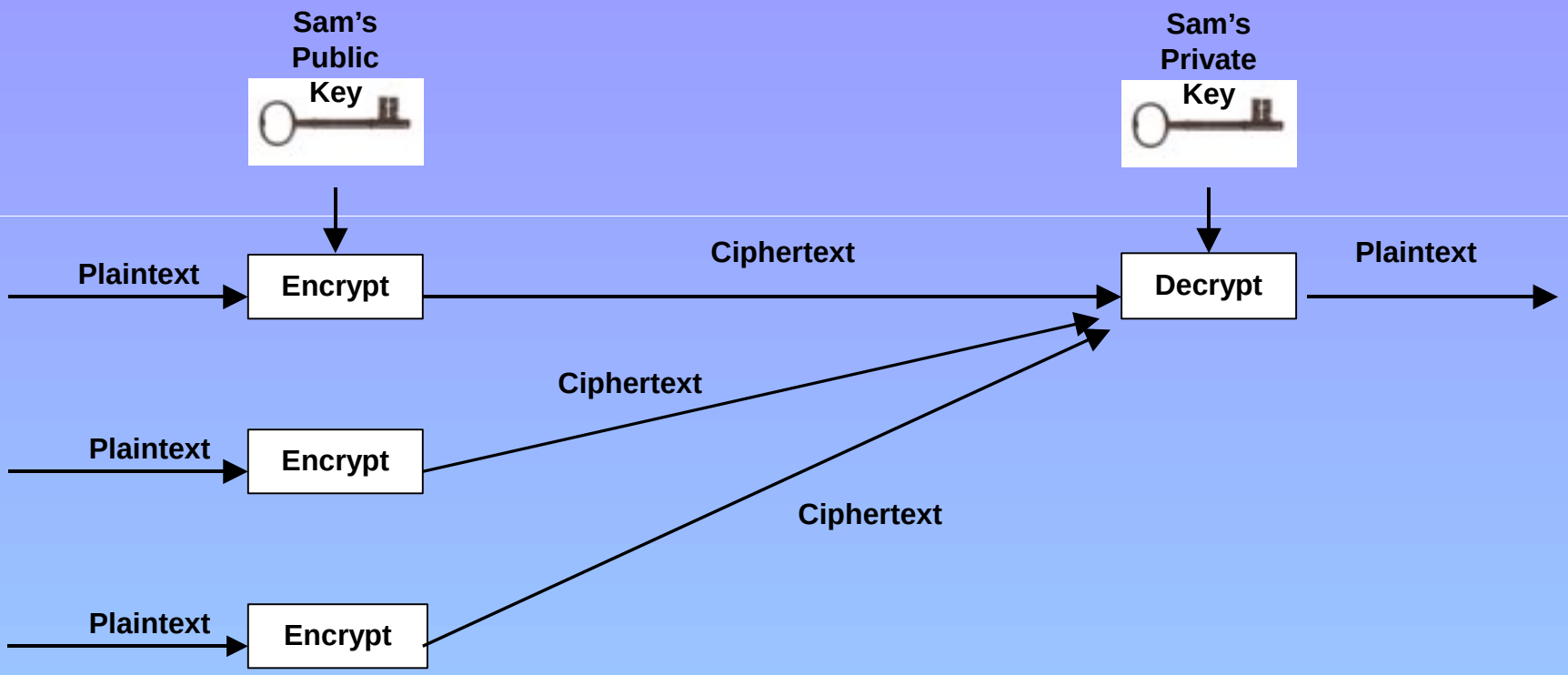
To build an electronic signature infrastructure, the state has:

- Policy Authority establishing the ground rules (Office of the Secretary of State).
- Certification Authority registering the subscriber & issuing digital certificates (CA approved by Secretary of State).
- Agency contracting with the CA for services.
- Subscriber getting a certificate to have a digital signature.
- Relying Party verifies the digital signature received from the subscriber.

# The Roles in Electronic Signature Use
# (State of Arizona's infrastructure model)

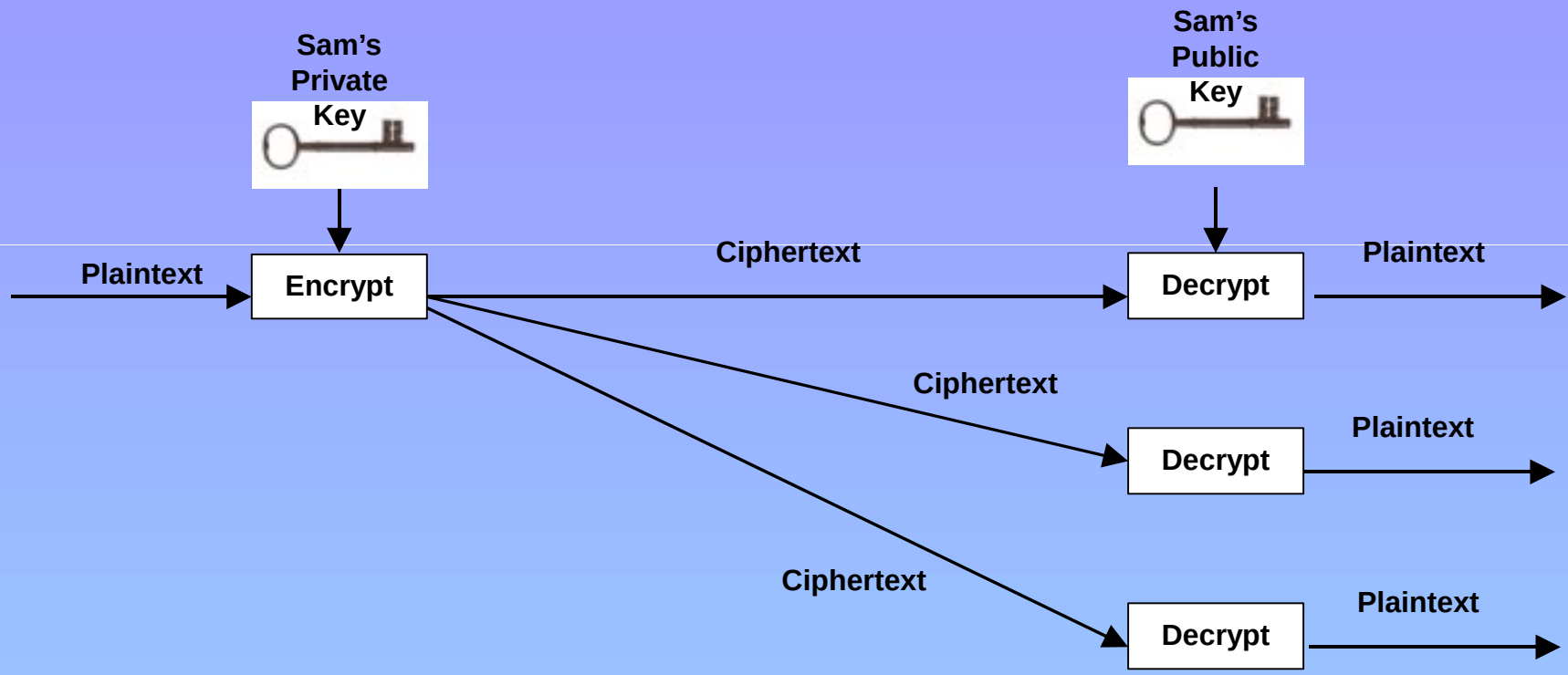


A fast history lesson -
the first idea of public/private key use was for encryption.
(eliminated the problems with shared secret encryption)



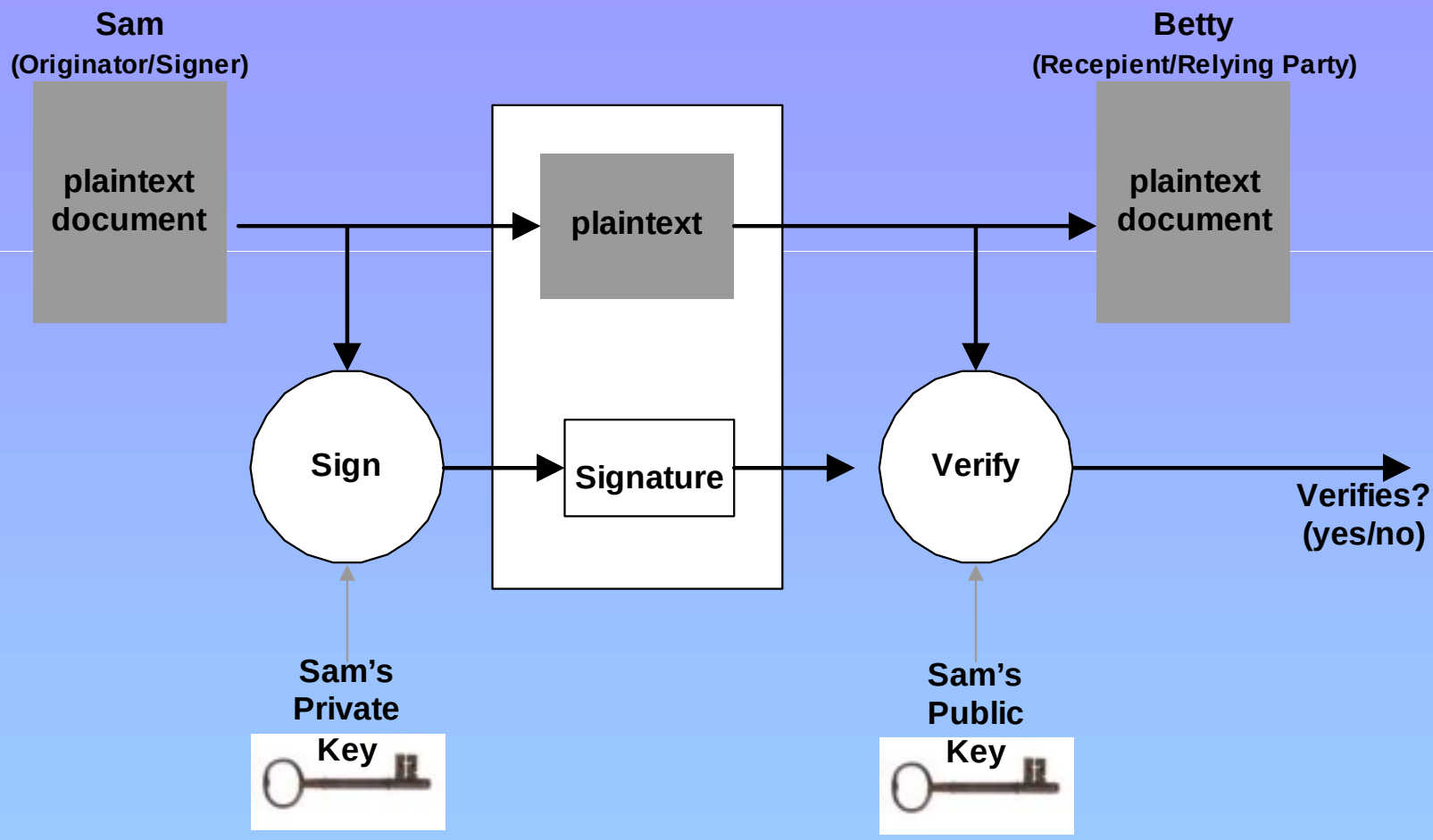

Several people can encrypt and send secure messages to Sam.
And only Sam can read them.
**This is "Hi, only you can read this."**
(aka PKC - Public Key Cryptography)

Then it was noticed
that switching the order of public/private key use led to identification.




Sam can encrypt and send *unsecure* messages to several people.
*But* they know it is *from* Sam.
**This is "Hi, it's really me." (Internet Caller ID)**

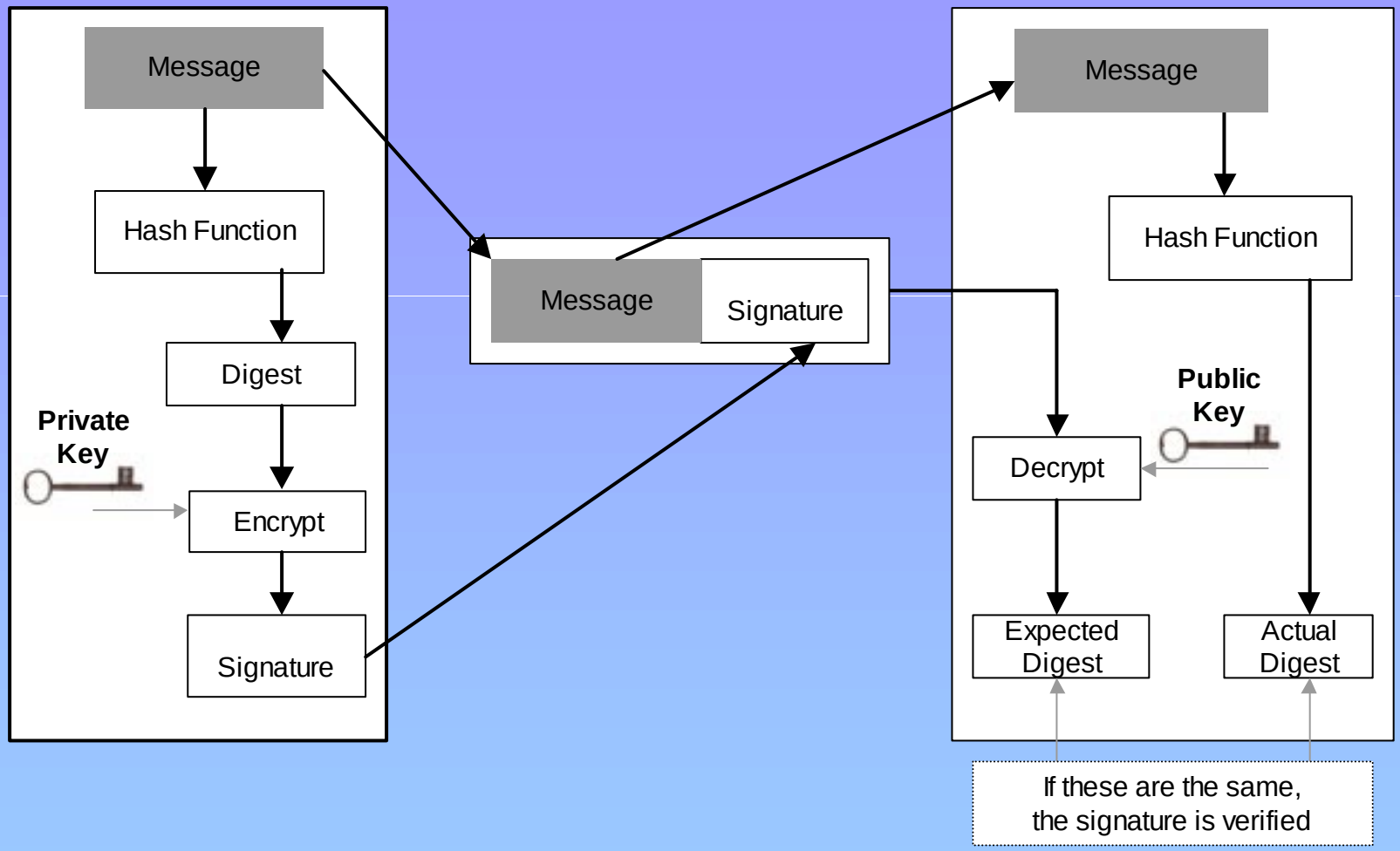
# Lightbulb -




Sam can send a message to Jean, who will know it is from Sam.

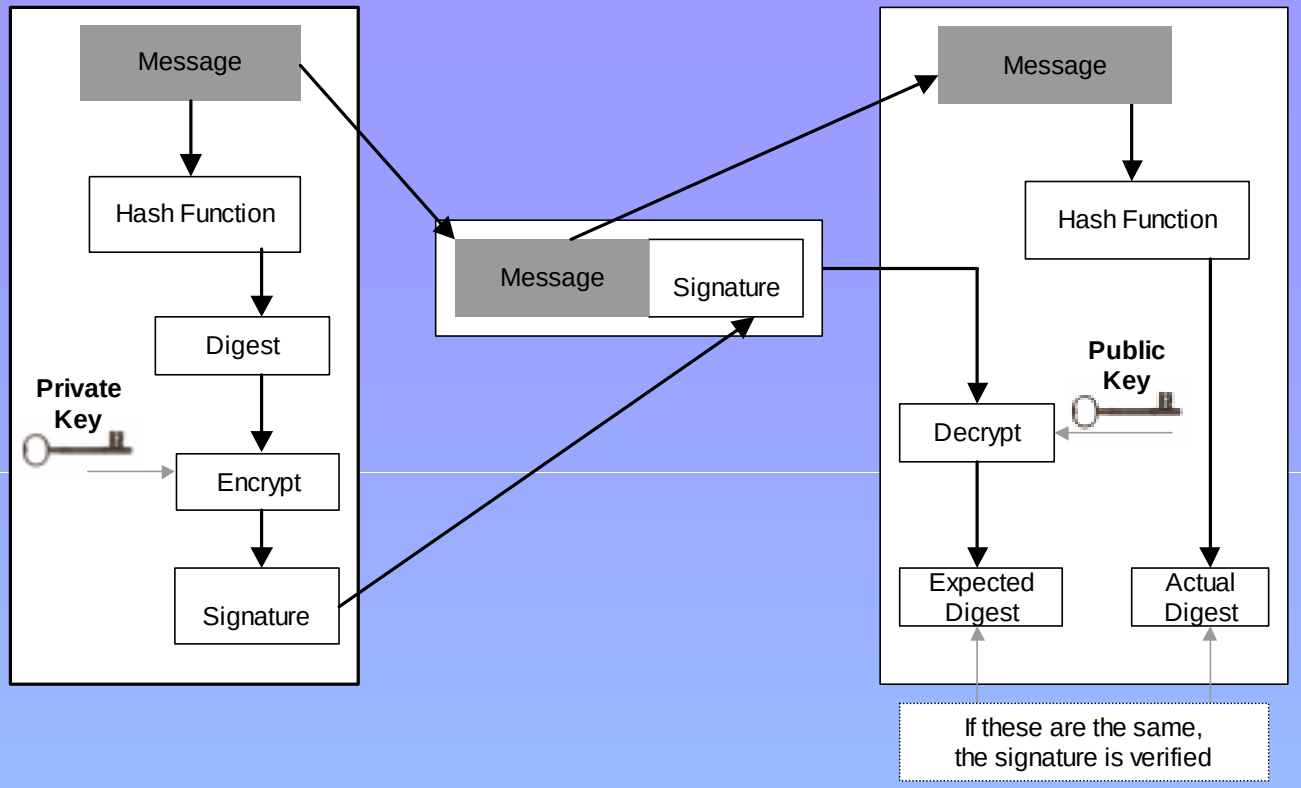
**This is "Hi, I sent this (but somebody might have changed it).**

To solve the risk
of a party between sender and receiver *changing* the message.




Sam can send a message to Jean. Jean will know it is from Sam and that the message has not been altered.

**This is "Hi, I sent this and you know whether it was changed.**




An electronic signature

shall be unique to the person using it,

shall be capable of reliable verification and

shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

Arizona Statute 41-132 B

## The need for Multi-jurisdictional Interoperability

*We understand paper and ink, and*
*we have standards - 8 1/2 x 11 inches, "permanent" ink, etc.*

*But we have open questions on the electronic equivalents of these:*

*How do we "read" electronic documents filed with us*
*by the private sector or by other jurisdictions?*
*How do we store, retrieve and forward those documents?*
*How do we know the next jurisdiction will accept them?*

## *E-SIGN Interoperability workgroup*

### *Vision Statement*

*December 2000*

E-SIGN: "Electronic Signatures in Global and National Commerce Act."

"Using electronic signatures means creating signed electronic documents. This forum will begin by asking 'how do we get from technology neutral e-signatures statutes to agreement about what are sharable, trustworthy signed electronic documents (things that are reliable, usable, authentic, and having integrity)?'"

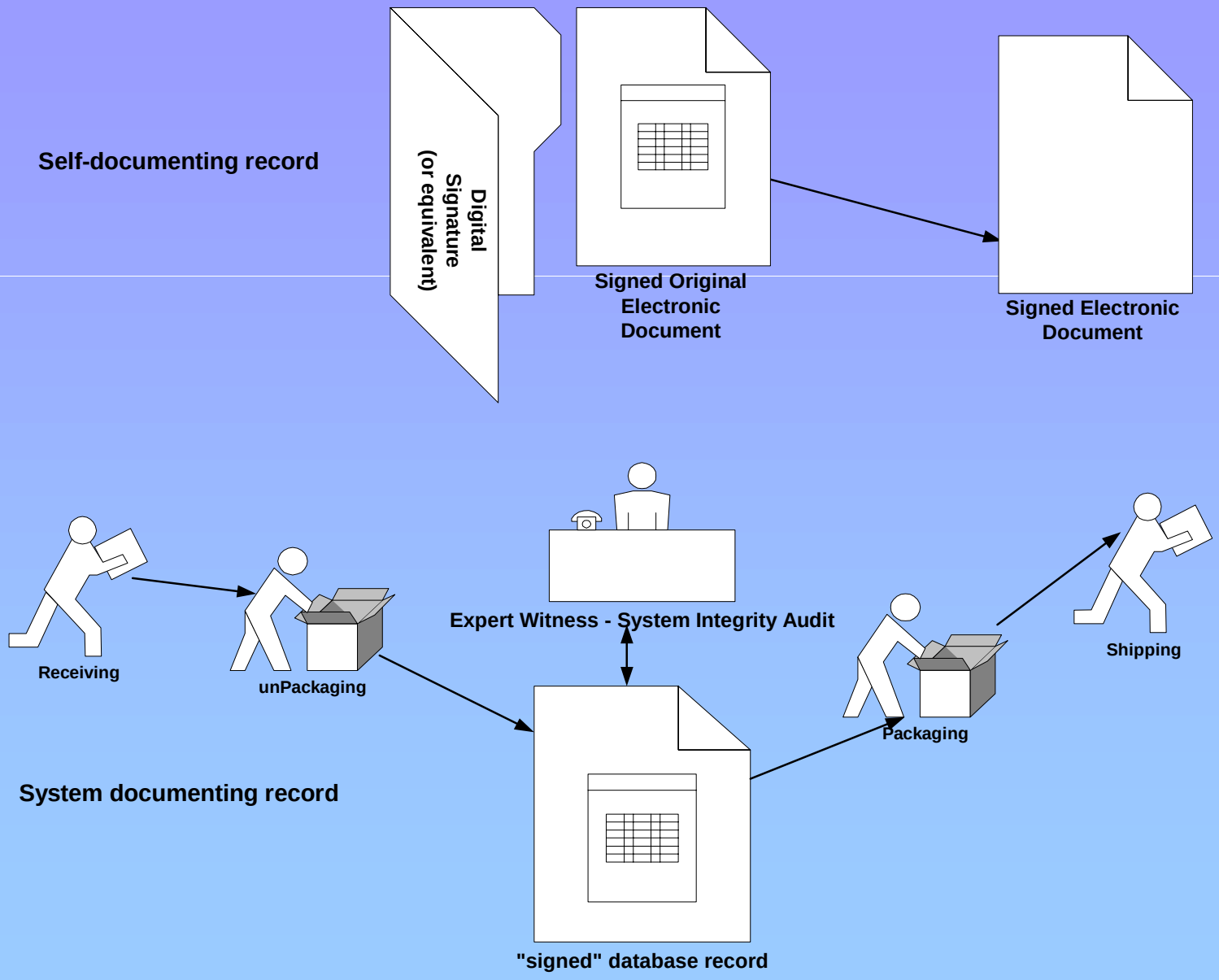
The group has developed a Trust Framework for electronic signatures and is currently working on a model Certificate Policy. The internal review and comment process should be complete by mid summer.

---

This workgroup is one of four created as a joint venture between the National Governors' Association (NGA) and National Electronic Commerce Coordinating Council (NECCC) to address the issues arising from the recently enacted *Electronic Signatures in Global and National Commerce Act* (E-SIGN) and *Uniform Electronic Transactions Act* (UETA) legislation.

*E-SIGN related multi-state Initiatives*

# different Trust Policies for different processes



*Electronic Signatures Framework for multi-state Interoperability*

- fully self-documented electronic record (e.g. PKI/XML)
  *relatively unique, relatively open*
  (evidence based on test of record)

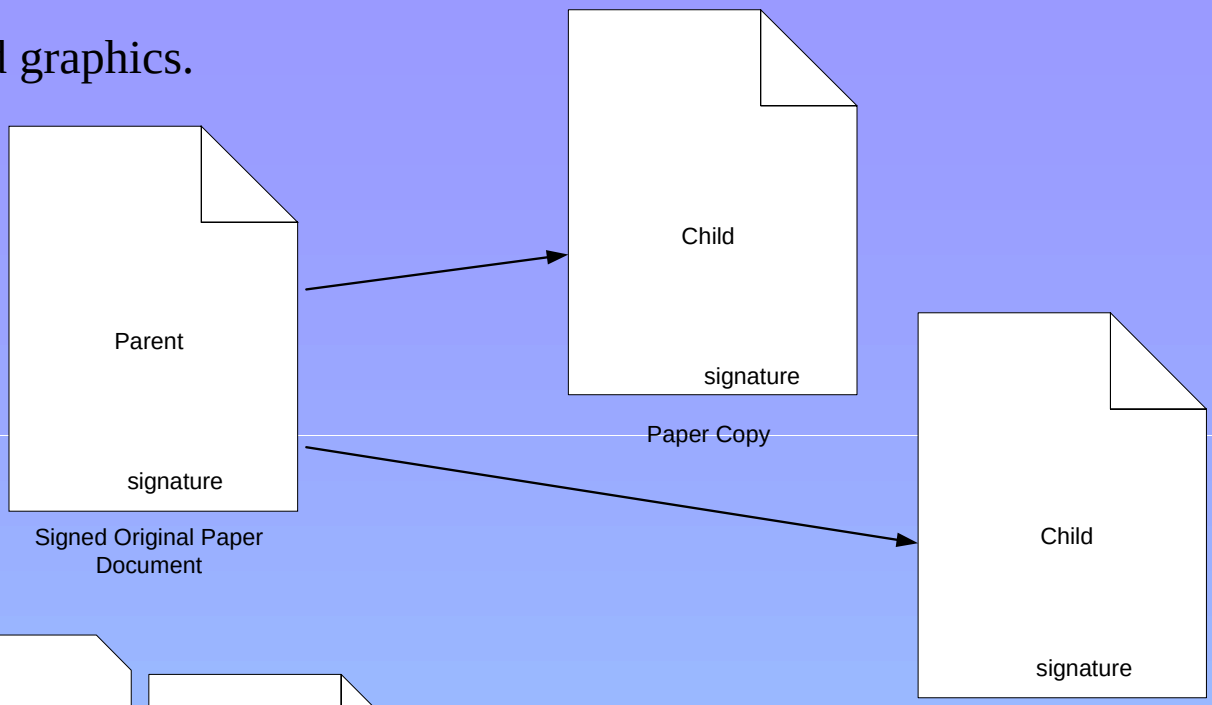
- fully trustworthy document system (e.g. EDI)
  does not have self-documented electronic records
  *could be problematic unless truly closed system*
  (evidence based on testimony about the system)

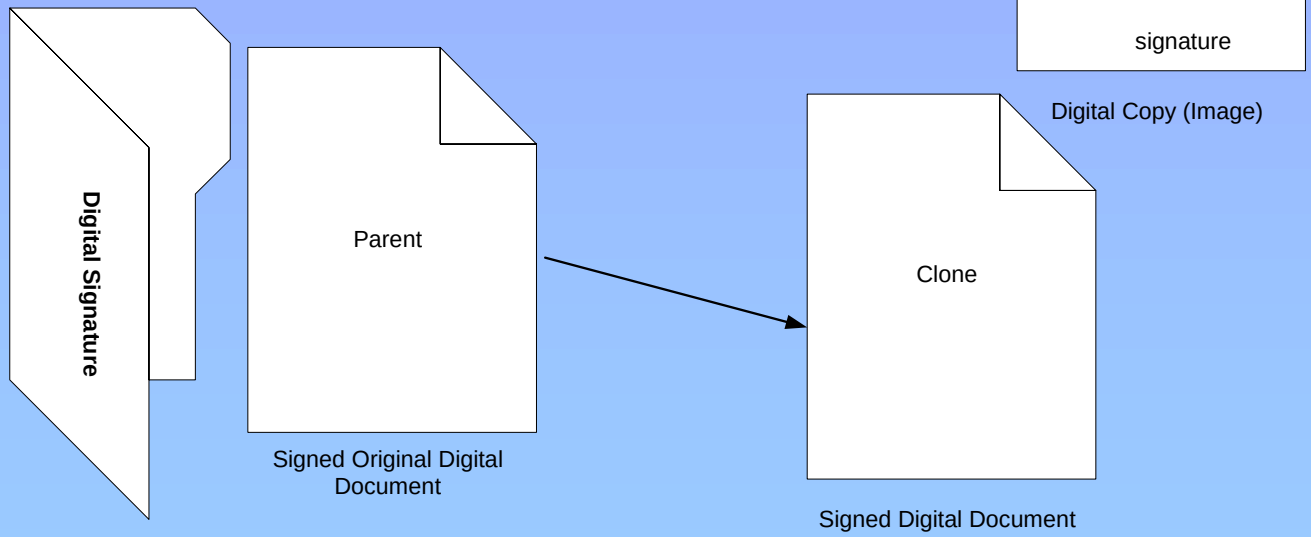
- fully self-documented electronic record *in*
  a fully trustworthy document system (e.g. PKI/XML/EDI)
  *generally a series,*
  *relatively closed but readily exported to open system use*

- fully trustworthy document system
  does not have self-documented electronic records *but*
  can reliably export a self-documented electronic record
  *generally a series,*
  *relatively closed but exportable to open system use*

***Notarization or certified copy can bridge incompatible document systems.***

On Paper -
The “document” is text and graphics.




On Digital -
The “document” is *anything digital* - text, graphics, sound, audio-video - anything that can be stored in a digital form and verifiably “replayed” in a human understandable form.

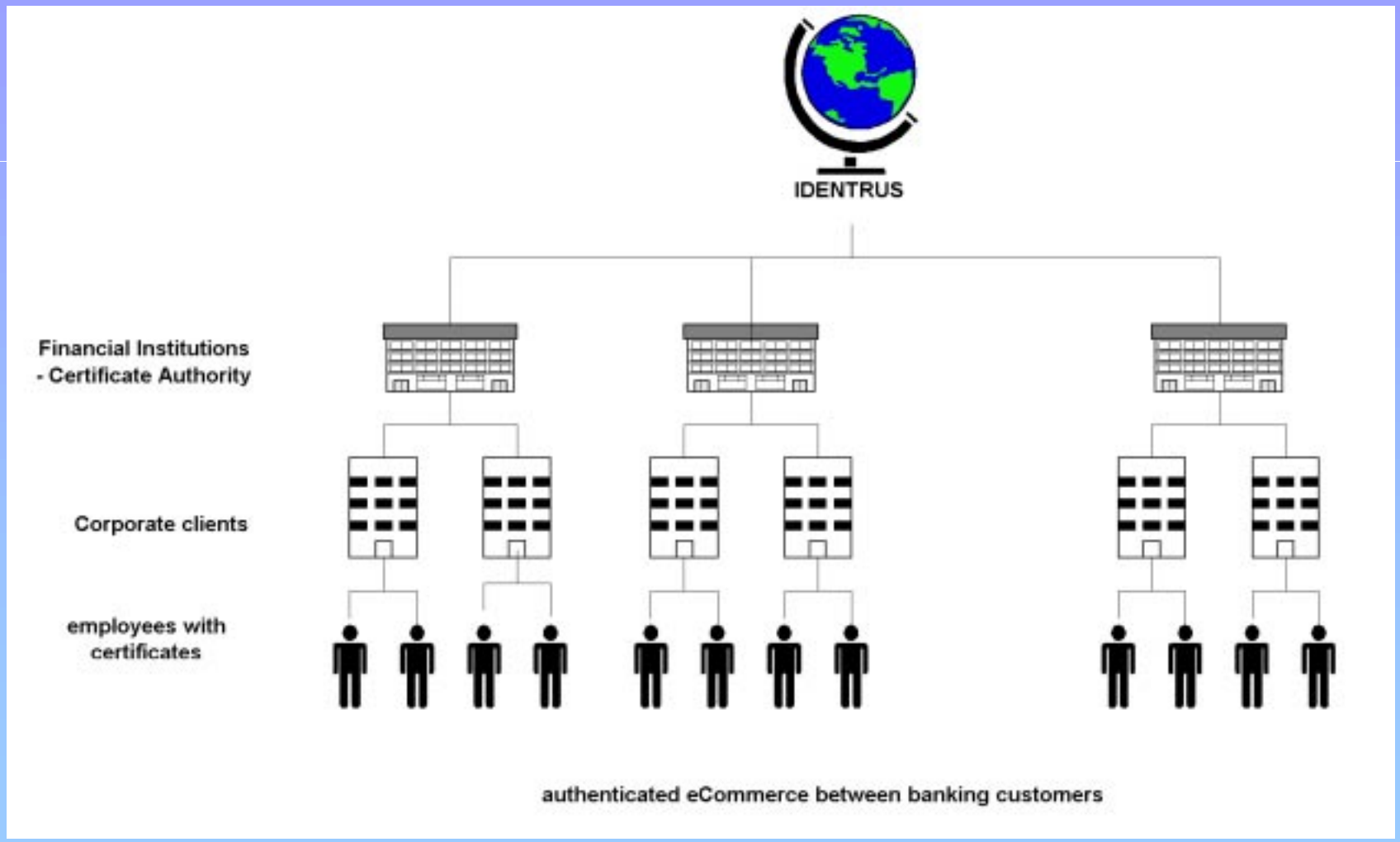
# CyberSpace - the new frontier

- Contract law still applies
- Rules of evidence still apply
- The evidence is different
  - On paper you sign and make copies,
    in cyberspace you sign and make clones (duplicate originals)
  - The evidence of tampering with an electronic document is different from the evidence of tampering with a paper one.
- An electronic signature *is not* a digital image of a handwritten signature

  (a digital image may be *part* of an electronic signature process
  but it is not sufficient in and of itself)

# Identrus

## an international banking trust initiative via an interoperable PKI network



## Summary

One reason for spending some time on “why a signature” and “what is an electronic document” was to build a foundation for determining what is appropriate for what circumstance - what will hold up as evidence of a “legal” signing of a “legal” document.

**Transactions are Transactions,**
**Contracts are Contracts,**
**but Everything Else Changes**

Mike Totherow
Chief Information Officer
Arizona’s Office of the Secretary of State
mtotherow@sos.state.az.us
602.542.6170

Russ Savage
Electronic Transactions Liaison
Arizona’s Office of the Secretary of State
rsavage@sos.state.az.us
602.542.2022